Catálogo de Especialidades Formativas

PROGRAMA FORMATIU

Implantació i gestió de la ciberseguretat

Setembre 2021

GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE

SISTEMA NACIONAL DE EMPLEO

IDENTIFICACIÓ DE L'ESPECIALITAT I PARÀMETRES DEL CONTEXT FORMATIU

Denominació de lespecialitat:	IMPLANTACIÓ I GESTIÓ DE LA CIBERSEGURETAT
Família Professional:	INFORMÀTICA I COMUNICACIONS
Àrea Professional:	SISTEMES I TELEMÀTICA
codi:	IFCT123
Nivell de qualificació professional:	4

Objectiu general

Gestionar les eines i els procediments de protecció dels sistemes d'informació contra ciberatacs o accessos no autoritzats.

Relació de mòduls de formació

Mòdul 1	Protecció i detecció datacs.	25 hores
Mòdul 2	Eines bàsiques de prevenció	18 hores
Mòdul 3	Control d'accés d'usuaris i aplicacions	18 hores
Mòdul 4	Eines de gestió de processos de recuperació	20 hores
Mòdul 5	Plans d'instal·lació i operació de sistemes de gestió de la ciberseguretat	10 hores

Modalitats d´impartició

Presencial

Teleformació

Durada de la formació

Durada total a qualsevol modalitat d'impartició	91 hores

Teleformació Durada total de les tutories presencials: 10 hores

Requisits daccés de lalumnat

Acreditacions / titulacions	Complir com a mínim algun dels requisits següents: - Títol de Grau o equivalent - Títol de Postgrau (Master) o equivalent - Títol de Tècnic Superior (FP Grau Superior) o equivalent de la família professional Informàtica i Comunicacions - Certificat de professionalitat de nivell 3 de la família professional Informàtica i Comunicacions

Experiència professional	En cas de no disposar dacreditació/titulació es requerirà una experiència professional mínima de 2 anys en tasques relacionades amb la gestió de xarxes o sistemes informàtics.
Modalitat de teleformació	A més del que s'ha indicat anteriorment, l'alumnat ha de tenir les destreses suficients per ser usuaris de la plataforma virtual on es recolza l'acció formativa.

Justificació dels requisits de lalumnat

Per acreditar els coneixements adquirits serà suficient aportar el justificant d'haver finalitzat els estudis, o el resguard d'haver-ho sol·licitat, o l'expedient acadèmic dels estudis realitzats.

En cas de requerir la justificació de lexperiència laboral, lalumnat haurà daportar un certificat de lempresa, indicant les tasques a què sha dedicat i el percentatge de la jornada laboral dedicat a les tasques relacionades amb la formació que ens ocupa.

Prescripcions de formadors i tutors

Acreditació requerida	Complir com a mínim algun dels requisits següents: - Llicenciat, enginyer, màster en alguna especialitat TIC relacionada amb aquesta formació, o el títol de grau corresponent o altres títols equivalents. - Diplomat, Enginyer Tècnic, o el títol de Grau corresponent o altres títols equivalents. - Tècnic superior de la família professional d'informàtica i Comunicacions.
Experiència professional mínima requerida	Es requeriran 2 anys dexperiència en tasques relacionades amb els temes abordats en aquesta formació.
competència docent	Experiència docent o investigadora acreditable a l'àmbit de la ciberseguretat, d'almenys 60 hores en modalitat presencial
Modalitat de teleformació	A més de complir les prescripcions establertes anteriorment, els tutors-formadors han d'acreditar una formació mínima de 30 hores, o experiència mínima de 60 hores, en aquesta modalitat i en la utilització de les tecnologies de la informació i comunicació.

Justificació de les prescripcions de formadors i tutors

Els formadors han dacreditar la seva titulació i aportar alguna justificació de docència impartida en la modalitat triada.

Requisits mínims d'espais, instal·lacions i equipaments

Espais formatius	superfície m2 per a 15 participants	increment Superfície / participant (Màxim 30 participants)
Aula de gestió	45 m2	2,4 m2 / participant

Espai Formatiu	Equipament
Aula de gestió	- Taula i cadira pel formador - Taules i cadires per a lalumnat - Material d'aula - pissarra - PC instal·lat en xarxa amb possibilitat d'impressió de documents, canó amb projecció i Internet pel formador - PC instal·lats en xarxa i Internet amb possibilitat d'impressió per als alumnes. - Programari específic per a laprenentatge de cada acció formativa: ÿ Sistema operatiu Windows ÿ Plataforma per a l'execució de sistemes i aplicacions virtualitzades ÿ Eina de SIEM

La superfície dels espais i les instal·lacions estaran en funció de la seva tipologia i del nombre d'alumnes. Tindran com a mínim els metres quadrats que s'indiquen per a 15 alumnes i l'equipament suficient per a aquests.

En cas que augmenti el nombre d'alumnes, fins a un màxim de 30, la superfície de les aules s'incrementarà proporcionalment (segons s'indica a la taula respecte a m2 /alumne) i l'equipament estarà d'acord amb aquest augment.

Les instal·lacions i els equipaments han de complir la normativa industrial i higiènic sanitària corresponent i han de respondre a mesures d'accessibilitat i seguretat de l'alumnat.

En cas que la formació s'adreci a persones amb discapacitat es faran les adaptacions i els ajustos raonables per assegurar-ne la participació en condicions d'igualtat.

Aula virtual

Si s'utilitza l'aula virtual s'han de complir les indicacions següents:

• **Característiques**
- La impartició de la formació mitjançant aula virtual s'ha d'estructurar i organitzar de manera que es garanteixi en tot moment que hi hagi connectivitat sincronitzada entre les persones formadores i l'alumnat participant així com bidireccionalitat a les comunicacions. - Cal comptar amb un registre de connexions generat per l'aplicació de l'aula virtual en què s'identifiqui, per a cada acció formativa desenvolupada a través d'aquest mitjà, les persones participants a l'aula, així com les dates i els temps de connexió.

Si l'especialitat s'imparteix en **modalitat de teleformació,** quan hi hagi tutories presencials, s'utilitzaran els espais formatius i els equipaments necessaris indicats anteriorment.

Per impartir la formació en **modalitat de teleformació,** cal disposar del següent equipament.

Plataforma de teleformació:

La plataforma de teleformació que s'utilitzi per impartir accions formatives ha d'allotjar el material virtual d'aprenentatge corresponent, tenir prou capacitat per desenvolupar el procés d'aprenentatge i gestionar i garantir la formació de l'alumnat, permetent la interactivitat i el treball cooperatiu, i reunir els següents requisits tècnics d'infraestructura, programari i serveis:

• **Infraestructura**

- Tenir un rendiment, entès com a nombre dalumnes que suporti la plataforma, velocitat de resposta de servidor als usuaris, i temps de càrrega de les pàgines web o de descàrrega darxius,

que permeti:

a) Suportar un nombre d'alumnes equivalent al nombre total d'alumnat en les accions formatives de formació professional per a l'ocupació que estigui impartint el centre o entitat de formació, garantint un allotjament mínim igual al total de l'alumnat d'aquestes accions, considerant que el número màxim dalumnes per tutor és de 80 i un nombre dusuaris concurrents del 40% daquest alumnat.

b) Disposar de la capacitat de transferència necessària perquè no es produeixi efecte retard en la comunicació audiovisual en temps real, havent de tenir el servidor on s'allotja la plataforma una amplada de banda mínima de 300 Mbs, suficient en baixada i pujada.

- Estar en funcionament 24 hores al dia, els 7 dies de la setmana.

• Programari:

- Compatibilitat amb l'estàndard SCORM i els paquets de continguts IMS.

- Nivells daccessibilitat i interactivitat dels continguts disponibles mitjançant tecnologies web que almenys compleixin les prioritats 1 i 2 de la Norma UNE 139803: 2012 o posteriors actualitzacions, segons el que estipulen el capítol III del Reial decret 1494/2007, de 12 de novembre.

- El servidor de la plataforma de teleformació ha de complir els requisits que estableix la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, per la qual cosa el responsable d'aquesta plataforma ha d'identificar la localització. física del servidor i el compliment del que estableixen transferències internacionals de dades en els articles 40 a 43 de l'esmentada Llei Orgànica 3/2018, de 5 de desembre, així com, en allò que sigui aplicable al Reglament (UE) 2016/679 del Parlament Europeu i de Consell, de 27 d'abril del 2016, relatiu a la protecció de les persones físiques respecte del tractament de dades personals i la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE.

- Compatibilitat tecnològica i possibilitats dintegració amb qualsevol sistema operatiu, base de dades, navegador dInternet dels més usuals o servidor web, havent de ser possible utilitzar les funcions de la plataforma amb complements (plug-in) i visors compatibles. Si es requereix la instal·lació addicional d'algun suport per a funcionalitats avançades, la plataforma ha de facilitar-ne l'accés sense cost.

- Disponibilitat del servei web de seguiment (operatiu i en funcionament) de les accions formatives impartides, d'acord amb el model de dades i protocol de transmissió establerts a l'annex V de l'Ordre/TMS/369/2019, de 28 de març.

• Serveis i suport

- Sustentar el material virtual d'aprenentatge de l'especialitat formativa que a través d'aquesta imparteixi.

- Disponibilitat d'un servei d'atenció a usuaris que doni suport tècnic i mantingui la infraestructura tecnològica i que, de manera estructurada i centralitzada, atengui i resolgui les consultes i les incidències tècniques de l'alumnat. Les maneres d'establir contacte amb aquest servei, que seran mitjançant telèfon i missatgeria electrònica, han d'estar disponibles per a l'alumnat des de l'inici fins a la finalització de l'acció formativa, mantenint un horari de funcionament del matí i de vesprada i un temps de demora a la resposta no superior a 48 hores laborables.

- Personalització amb la imatge institucional de l'administració laboral corresponent, amb les pautes d'imatge corporativa que s'estableixin.

A fi de gestionar, administrar, organitzar, dissenyar, impartir i avaluar accions formatives a través d'Internet, la plataforma de teleformació integrarà les eines i els recursos necessaris per a aquesta finalitat, disposant, específicament, d'eines de:

- Comunicació, que permetin que cada alumne pugui interaccionar a través del navegador amb el

tutor-formador, el sistema i amb els altres alumnes. Aquesta comunicació electrònica s'ha de fer mitjançant eines de comunicació síncrones (aula virtual, xat, pissarra electrònica) i asíncrones (correu electrònic, fòrum, calendari, tauler d'anuncis, avisos). És obligatori que cada acció formativa en modalitat de teleformació disposi, com a mínim, d'un servei de missatgeria, un fòrum i un xat.

- Col·laboració, que permetin tant el treball cooperatiu entre els membres dÿun grup, com la gestió de grups. Mitjançant aquestes eines ha de ser possible realitzar operacions d'alta, modificació o esborrament de grups d'alumnes, així com crear “escenaris virtuals” per al treball cooperatiu dels membres d'un grup (directoris o “carpetes” per a l'intercanvi d'arxius, eines per a la publicació dels continguts, i fòrums o xats privats per als membres de cada grup).

- Administració, que permetin la gestió dusuaris (altes, modificacions, esborrament, gestió de la llista de classe, definició, assignació i gestió de permisos, perfils i rols, autenticació i assignació de nivells de seguretat) i la gestió daccions formatives.

- Gestió de continguts, que possibiliten l'emmagatzematge i la gestió d'arxius (visualitzar arxius, organitzats en carpetes -directoris- i subcarpetes, copiar, enganxar, eliminar, comprimir, descarregar o carregar arxius), la publicació organitzada i selectiva dels continguts de aquests arxius, i la creació de continguts.

- Avaluació i control del progrés de lalumnat, que permetin la creació, edició i realització de proves davaluació i autoavaluació i dactivitats i treballs avaluables, la seva autocorrecció o la seva correcció (amb retroalimentació), la seva qualificació, assignació de puntuacions i la ponderació de les mateixes, el registre personalitzat i la publicació de qualificacions, la visualització dinformació estadística sobre els resultats i el progrés de cada alumne i lobtenció dinformes de seguiment.

Material virtual d'aprenentatge:

El material virtual d'aprenentatge per a l'alumnat mitjançant el qual s'imparteixi la formació es concretarà al curs complet en format multimèdia (que mantingui una estructura i funcionalitat homogènia), i s'hauran d'ajustar a tots els elements de la programació (objectius i resultats d'aprenentatge) d'aquest programa formatiu que figura al Catàleg d'Especialitats Formatives i el contingut compleixi aquests requisits:

- Com a mínim, ser l'establert a l'esmentat programa formatiu del Catàleg de Especialitats formatives.
- Estar referit tant als objectius com als coneixements/capacitats cognitives i pràctiques, i habilitats de gestió, personals i socials, per la qual cosa en conjunt permetin aconseguir els resultats d'aprenentatge previstos.

- Organitzar-se a través d'índexs, mapes, taules de contingut, esquemes, epígrafs o titulars de fàcil discriminació i seqüenciats pedagògicament de manera que en permeten la comprensió i la retenció.

- No va ser merament informatius, promovent la seva aplicació pràctica a través d'activitats d'aprenentatge (autoavaluables o valorades pel tutor-formador) rellevants per a l'adquisició de competències, que serveixin per verificar el progrés de l'aprenentatge de l'alumnat, fer-ne un seguiment de les dificultats daprenentatge i prestar-li el suport adequat.

- No va ser exclusivament textuals, incloent-hi variats recursos (necessaris i rellevants), tant tàtics com interactius (imatges, gràfics, àudio, vídeo, animacions, enllaços, simulacions, articles, fòrum, xat, etc.). de manera periòdica.
- Poder ser ampliats o complementats mitjançant diferents recursos addicionals a què l'alumnat pugui accedir i consultar a voluntat.
- Donar lloc a resums o síntesis i glossaris que identifiquin i defineixin els termes o vocables sics, rellevants o claus per a la comprensió dels aprenentatges.
- Avaluar la seva adquisició durant ia la finalització de lacció formativa a través dactivitats davaluació (exercicis, preguntes, treballs, problemes, casos, proves, etc.), que permeten mesurar el rendiment o lexercici de lalumnat.

Altres especificacions

Tecnologia i equips	- La plataforma de teleformació inclourà una eina que permeti la connexió síncrona de docents i alumnes, amb sistema incorporat dàudio, vídeo i possibilitat de compartir arxius, la pròpia pantalla o altres aplicacions tant pel docent com per lalumnat, amb registre dels temps de connectivitat.

Ocupacions i llocs de treball relacionats

- 27191013 Auditors-assessors informàtics
- 2711 Analistes de sistemes
- 2723 Analistes de xarxes informàtiques
- 27231014 Analistes i desenvolupadors de xarxes informàtiques
- 2722 Administradors de sistemes i xarxes
- 3811 Tècnics en operacions de sistemes informàtics
- 3812 Tècnics en assistència a l'usuari de tecnologies de la informació
- 3813 Tècnics en xarxes
- 27111046 Enginyers tècnics en informàtica de sistemes
- 27191022 Enginyers tècnics en informàtica, en general

Requisits oficials de les entitats o centres de formació

Estar inscrit al Registre d'entitats de formació (Serveis Públics d'Ocupació)

DESENVOLUPAMENT MODULAR

MÒDUL DE FORMACIÓ 1: PROTECCIÓ I DETECCIÓ D'ATACS

OBJECTIU

Aplicar mesures de protecció als equips informàtics connectats a una xarxa corporativa.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 25 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS DE L'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Gestió d'incidents de ciberseguretat: Centre d'Operacions de Seguretat – SOC
  - El perill
  - Defensors a la guerra contra el delicte cibernètic
- Inspecció detallada dels atacs a través de la xarxa
  - Eines de supervisió del trànsit de xarxa
  - Vulnerabilitats i atacs al protocol
  - Vulnerabilitats i atacs als serveis
- Aplicació de mesures de protecció d'atacs
  - Mètodes d'intrusions en sistemes
  - Mètodes d'infeccions d'aplicacions
  - Eines per a la descoberta de nous patrons d'atac
  - Mètodes de detecció basats en signatura
  - Mètodes de detecció heurístics
  - Mètodes de detecció de comportament anormal

Habilitats de gestió, personals i socials

- Assimilació de les funcions i objectius del centre d'operacions de seguretat a la pre venció d'atacs de ciberseguretat a les xarxes.
- Consulta de les fonts d'informació sobre els atacs coneguts i les recomanacions de detecció i mitigació.
- Rigor en la selecció, la recomanació i l'automatització de les tasques d'instal·lació, la configuració i l'actualització de les eines de detecció i prevenció d'atacs.
- Valoració de les característiques i limitacions de cada tipus d'eina de protecció i detecció
- Organització dels equips de supervisió i detecció datacs.

MÒDUL DE FORMACIÓ 2: EINES BÀSIQUES DE PREVENCIÓ

OBJECTIU

Configurar les eines bàsiques de protecció del sistema informàtic.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 18 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS DE L'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Anàlisi dels Tallafocs
  - Principis de funcionament
  - Tipus de tallafocs: tradicionals, UTM (Unified Threat Management) i NGFW (Next Generation Firewall)
  - Polítiques de filtrat
  - Gestió i configuració de firewalls

- Aplicació de sistemes de protecció contra virus i codi maliciós (malware)
  - APT: Amenaces persistents avançades
  - Concepte d'EPP (Endpoint protecction platform)
  - Concepte d'EDR (Endpoint Detection and Response)
  - Gestió i configuració de sistemes EDR
  - Estratègies de configuració de sistemes de protecció als endpoints.
  - Exemples de sistemes EDR i EPP

Habilitats de gestió, personals i socials

- Sensibilització per seleccionar els tallafocs més adequats en la detecció dels tipus i patrons d'atac coneguts, tant a nivell de xarxa com d'aplicació.
- Valoració d'aplicació de polítiques de filtratge.
- Rigor en la selecció dels sistemes de protecció contra virus i programes maliciosos (Malware) més adequades per a les característiques del trànsit i documents gestionats a l'organització, en funció de les seves característiques funcionals i operatives.
- Coordinació en la gestió i configuració dels sistemes de protecció i detecció de programes maliciosos.

MÒDUL DE FORMACIÓ 3: CONTROL D'ACCÉS D'USUARIS I APLICACIONS

OBJECTIU

Planificar els mecanismes d'autenticació i autorització d'usuaris més adequats per evitar la suplantació d'identitat i/o accessos no autoritzats, des del disseny fins al manteniment.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 18 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS DE L'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Configuració de mecanismes de control d'accés i autenticació – Mètodes d'identificació dels usuaris (contrasenyes, biometria, etc.). ID digital i signatura-e. Riscos i beneficis de la ID digital

- Sistemes de gestió dels drets d'accés d'usuari: ACL, RBAC, PBAC
- Sistemes d'autenticació vs. autorització
- Sistemes de federació d'identitats: SSO
- Artefactes d'acreditació de drets d'accés (SAML)
- Procediments daltres i baixes dusuaris i privilegis.

• Anàlisi de propostes pràctiques de control d'accés a aplicacions –
Autenticació i autorització en serveis WEB.
- OAuth, OAuth2 i tokens.

Habilitats de gestió, personals i socials

• Avaluació des de riscos associats a potencials suplantadors d'identitat.

• Canalització de les necessitats dels usuaris de coneixement i gestió de les dades sensibles vinculades als processos de negoci de la corporació.

• Rigor en la selecció, la planificació i la implantació dels mecanismes d'autenticació més adequades per a cada aplicació i col·lectiu dusuaris.

• Responsabilitat en la redacció i el manteniment dels procediments de gestió de identitat dins de la corporació.

MÒDUL DE FORMACIÓ 4: EINES DE GESTIÓ DE PROCESSOS DE RECUPERACIÓ

OBJECTIU

Planificar els procediments de recuperació de dades i serveis de les corporacions, així com les eines més bàsiques per aconseguir-ho de forma eficient i efectiva, incloent-ne la validació.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 20 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS DE L'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

• Planificació de la recuperació i restauració de serveis després d'un incident
- Definició i implantació dels plans de recuperació, segons el tipus dincident i impacte
– Definició i implantació dels plans de restauració dels processos de negoci.
- Planificació i execució dexercicis de recuperació i restauració

• Gestió de les còpies de seguretat
- Tipus de còpies de seguretat, segons la freqüència i la ubicació de les còpies
- Eines d'automatització de processos de còpia
- Procediments i proves de recuperació de còpies
- Protecció de les còpies de seguretat
- Polítiques de còpies de seguretat

• Aplicació de ferramentes de configuració i manteniment remots
- Eines daccés remot a dispositius de sobretaula i portàtils.
- Eines d'accés remot a dispositius mòbils
- Capacitats dinstal·lació, control i configuració remotes.

Habilitats de gestió, personals i socials

- Negociació en la identificació dels processos de negoci crítics i dels components dels sistemes informàtics necessaris per al seu funcionament.
- Responsabilitat en el dimensionament dels recursos necessaris per a la recuperació dels processos de negoci de la corporació, i planificació de la posada en marxa en cas d'incident greu.
- Rigor en la configuració, planificació, manteniment i validació dels procediments de recuperació de dades.
- Col·laboració en la posada en marxa d'eines de manteniment remot de dispo tius i formació del personal en la utilització responsable.

MÒDUL DE FORMACIÓ 5:	PLANS D'INSTAL·LACIÓ I OPERACIÓ DE SISTEMES DE GESTIÓ DE LA CIBERSEGURETAT

OBJECTIU

Aplicar les eines i els processos necessaris per gestionar la seguretat dels sistemes d'informació.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 10 hores

Teleformació: Durada de les tutories presencials: 10 hores

RESULTATS DE L'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Detecció d'anomalies al trànsit d'una xarxa corporativa
  - Configuració d'una eina de supervisió del trànsit a la xarxa
  - Configuració d'una eina de detecció d'anomalies a la xarxa
- Detecció d'indicadors d'atac o d'incident
  - Reconeixement de patrons datac
  - Detecció d'intrusions i infeccions a les xarxes i sistemes corporatius
- Automatització de procediments
  - Instal·lació i configuració de les eines de protecció contra incidents.
  - Supervisió de funcionament i optimització deficiència
- Recuperació després d'un incident de seguretat informàtica
  - Planificació dels procediments i designació de responsabilitats
  - Posada en pràctica i validació dels procediments

Habilitats de gestió, personals i socials

- Col·laboració amb altres membres de l'organització en la definició, la planificació i la validació dels procediments de recuperació i restauració de serveis i processos de negoci.
- Rigor a la redacció d'informes de resultats.

Resultats que obligatòriament s'han d'adquirir en presencial

- Detecció d'anomalies al trànsit d'una xarxa corporativa
  - Configuració d'una eina de supervisió del trànsit a la xarxa
  - Configuració d'una eina de detecció d'anomalies a la xarxa
- Detecció d'indicadors d'atac o d'incident
  - Reconeixement de patrons datac
  - Detecció d'intrusions i infeccions a les xarxes i sistemes corporatius
- Automatització de procediments
  - Instal·lació i configuració de les eines de protecció contra incidents.
  - Supervisió de funcionament i optimització deficiència
- Recuperació després d'un incident de seguretat informàtica
  - Planificació dels procediments i designació de responsabilitats
  - Posada en pràctica i validació dels procediments

ORIENTACIONS METODOLÒGIQUES

La impartició de la docència es durà a terme complementant:

- Introducció de conceptes teòrics i metodològics
- Estudi de casos en què s'hagin aplicat aquests
- Realització d'exercicis pràctics per demostrar les capacitats adquirides.

AVALUACIÓ DE L'APRENENTATGE A L'ACCIÓ FORMATIVA

- L'avaluació tindrà un caràcter teoricopràctic i es realitzarà de forma sistemàtica i contínua, durant el desenvolupament de cada mòdul i al final del curs. A les avaluacions programades es poden agrupar coneixements de diversos mòduls.
- Es realitzarà una avaluació inicial de caràcter diagnòstic per detectar el nivell de partida del alumnat.
- L'avaluació es durà a terme mitjançant els mètodes i els instruments més adequats per comprovar els diferents resultats d'aprenentatge, i que en garanteixin la fiabilitat i la validesa.
- Cada instrument d'avaluació s'acompanyarà del corresponent sistema de correcció i puntuació en què s'expliciti, de manera clara i inequívoca, els criteris de mesurament per avaluar els resultats aconseguits pels alumnes.
- La puntuació final aconseguida s'expressarà en termes d'apte/no apte.